[redacted]

Redacted Version

IN THE UNITED STATES COURT OF FEDERAL CLAIMS
BID PROTEST

AMAZON WEB SERVICES, INC.,	)	[redacted]
	)	
Plaintiff,	)	
	)	
v.	)	No. 19-1796C
	)	(Judge Patricia E. Campbell-Smith)
THE UNITED STATES,	)	
	)	[redacted]
Defendant,	)	
	)	
and	)	
	)	
MICROSOFT CORPORATION,	)	
	)	
Intervenor-Defendant.	)	

DECLARATION OF MS. SHARON WOODS

I, Sharon Woods, DoD, declare as follows:

1. I am the Director and Program Manager (PM) for the Cloud Computing Program Office (CCPO) within the office of the Chief Information Officer (CIO) for the Department of Defense (DoD). My responsibilities include acquisition and deployment of enterprise cloud services for DoD.

2. As the PM for CCPO, which is responsible for implementation of the Joint Enterprise Defense Infrastructure (JEDI) Cloud, I am familiar with the JEDI Cloud contract and can explain the harm to the department if DoD is unable to continue performance under this contract.

[redacted]

3. The mission of CCPO is to rapidly and securely deploy enterprise cloud services to DoD at all classification levels, from the home-front to the tactical edge. DoD and our national security will be significantly harmed by delayed implementation of JEDI's unclassified services. As explained below, there are multiple dependencies between the deployment of unclassified and classified services, meaning that if unclassified services are delayed, classified services are also delayed. Moreover, JEDI will satisfy critical needs for national security that are unmet by other available contracts.

4. While a majority of DoD's mission critical needs operate at the classified level, there are several critical dependencies between classified and unclassified services.

A. First, with regard to modern software development, there is an extremely limited pool of vendors with the necessary security clearances to develop software in classified environments, and clearing vendors is a slow, expensive process. To solve this problem, JEDI provides for secure movement of software and data up and down classification levels. This Cross Domain Solution (CDS), unique to JEDI, will allow users to achieve secure data transfer across different classification levels. JEDI's CDS capabilities solve the modern software development conundrum -- non-traditional contractors will develop software at the unclassified level, and then DoD can move that software up to Secret (and/or Top Secret) using CDS. For example, both the Joint Artificial Intelligence Center (JAIC) and Project Maven will be able to place task orders for unclassified services to begin software development activities immediately at "Go Live", currently anticipated for February 14, 2020. While Secret services will not be available immediately, those early adopters will need the interim period to

produce software that is ready to utilize the CDS when the Secret environment is launched. Delaying deployment of JEDI's unclassified services will delay software development work that must *first* occur in the unclassified JEDI environment.

B. Another critical dependency between classified and unclassified services relates to protection of classified information in the areas of user provisioning and tactical edge. Even with an awarded contract, cloud users cannot simply go online and sign up for cloud accounts; a contracting officer must first place a task order with certified funding and approval from a security officer. The result is a gap between DoD contracting systems and a vendor's online cloud portal. Most cloud contracts currently available to DoD address this gap manually, which often adds weeks or months to the ordering process. The potential security implications of mishandling this process are enormous.[1] To solve this important process gap, CCPO awarded a separate contract in March 2018 to a software developer to develop a provisioning tool that automates this process gap in a manner that supports user authentication and security auditing.

Critically, the activities of early adopters will operationally validate the functioning of the provisioning tool, in particular its security-related features and reporting and auditing capabilities. For security reasons, DoD cannot deploy the provisioning tool into the classified environment until, at the unclassified level, the tool is thoroughly validated as functioning properly and the reporting and

[1] For example, the Central Intelligence Agency (CIA) did not automate provisioning when it first launched Commercial Cloud Services (C2S), and expressed to DoD that its failure to do so earlier was one of its most significant lessons learned.

[redacted]

auditing capabilities are more mature. The 180 days between "Go Live" for the unclassified environment and "Go Live" for the classified environment is necessary to ensure reporting and auditing capabilities can be reliably validated. The proper functioning of these features is critical to mitigating insider security threats.

The same rationale applies to JEDI's tactical edge capabilities, which can operate in disconnected and austere environments. DoD has never deployed cloud-based tactical edge capabilities across the entire enterprise globally and at all classification levels. Ensuring that data on those devices is secure and properly synchronizes with the central cloud environment is technically complex, especially on such a large scale. Using early adopters, DoD will test and validate the functionality and security of unclassified tactical edge devices before authorizing and using classified tactical edge devices.

5. In her declaration accompanying AWS's Motion for Temporary Restraining Order and Preliminary Injunction, Jennifer Chronis cites to more than twenty cloud contracting vehicles, arguing that DoD would not suffer harm because those contracts are sufficient to meet DoD's cloud needs. It is true that there are many DoD contract vehicles covering cloud services, but the assertion that existing contracts can wholly meet DoD's current unclassified cloud computing needs intended to be addressed by JEDI is incorrect.

A. First, a majority of the available contract vehicles require task order level competitions, adding time and administrative burdens. In addition, of the contracts cited, all but two, C2S and GSA IT Schedule 70, are made available

[redacted]

through "cloud brokers."[2] Many of the cited contracts are also limited to particular communities, such as intelligence or specific military services. Likewise, most of the cited contracts have manual, not automated, ordering and provisioning processes.[3]

B. Importantly, none of the cited contracts provide services at all classification levels with integrated CDS capabilities. While there is access to limited tactical edge capabilities on select contracts, none of them approach the completeness of the JEDI solution and none of the cited contracts provide tactical edge capabilities that synchronize with the central cloud environment at all classification levels.

C. A less obvious, but equally critical reason that available contracts fail to meet DoD's unclassified requirements is related to commercial parity. Commercial parity, a fundamental underpinning of JEDI's requirements, means that DoD has the best, most advanced, most secure offerings available in the cloud marketplace. Until JEDI, this has not been achievable. JEDI will be the *only* DoD contract to date that allows for the use of *commercial* cloud services for controlled unclassified information (CUI) as opposed to separate GovCloud environments, which are less up-to-date and more costly.

6. AWS contends that it will be harmed if [redacted]

[redacted]

[2] "Cloud brokers" resell cloud capabilities for a price premium, along with migration and consulting services that fall outside the scope of the JEDI Cloud contract.

[3] Some available contracts have a degree of ordering automation, but the process can be extremely slow. The time between placing an order on these contracts and users provisioning accounts in the vendor's cloud portal can exceed 180 days depending on the contract.

[redacted]

A. [redacted]

B. [redacted]

C. [redacted]

[redacted]

7. [redacted]

8. Finally, if the result of this protest is that the JEDI contract is awarded to AWS in a subsequent re-compete, DoD would necessarily have to repeat all of the preparatory activities that led to Go Live. For the same reasons explained in this declaration, there are multiple, technically complex activities that must occur before DoD users will be allowed to use commercial cloud services for CUI or classified requirements. Likewise, under this scenario, early adopters would have to reassess what cloud environment would be most advantageous for any workloads already deployed in the Azure-based JEDI; being in the early stages of deployment, it is possible those early adopters would move their workloads to the AWS-based JEDI environment, especially considering the long-term stability and additional capabilities that are unique to JEDI.

I declare under penalty of perjury that the foregoing is true and correct. Executed on this 31 day of January, 2020.

WOODS.SHARON[redacted] Digitally signed by WOODS.SHARON[redacted] Date: 2020.01.31 09:30:15 -05'00'

SHARON WOODS
Director and Program Manager
Cloud Computing Program Office
Office of the Chief Information Officer
U.S. Department of Defense